(Approx. 836 words)

Wi-Fi Security – Protect your communications; don’t leave your Wi-Fi Open

By Phil Sorrentino, Contributing Writer, The Computer Club, FL

February 2019

www.scccomputerclub.org

Philsorr (at) yahoo.com

Wi-Fi is all around us. In homes, libraries, airports, shopping centers, recreational places, houses of worship, the CA buildings, just about everywhere. Wi-Fi is the first step in the complex way we get to the internet for information, entertainment, or purchases. Our smartphones, tablets, and computers, more than likely, communicate with a router over Wi-Fi. (I say more than likely because there are still some desktop computers directly connected to routers by wire, using an Ethernet RJ-45 connection). The router in turn connects to a modem (modulator-demodulator) which in turn connects to your ISP (internet service provider). It is the ISP that is the final step and the gateway to the internet and all of its wonderful websites and servers.

Wi-Fi is a wireless communications link. Like any wireless communications, for example radio or tv, it can be intercepted by an antenna and an appropriate receiver. This means that anyone with a laptop (antenna and receiver are integral components), and some special software (commonly called a wireless sniffer) could intercept the wireless signal and “listen in” on your digital communications. I don’t mean “listen in” as in hearing with your ears. I mean intercepting the digital data stream that makes up your communications, and interpreting, and possibly recording, the communications content. (Googling “sniffer” reveals that a network sniffer is a software tool that monitors, or sniffs out, the data flowing in a communications link in real time. It can be a self-contained software program or a hardware device with appropriate software or firmware. Wireshark is widely recognized as the world’s most popular network sniffer. It is a free, open source application that displays intercepted communications data. In the hands of a skilled user it can intercept communications and even capture passwords from nearby communications activity.) With this computer setup, the person at the next table at your favorite coffee shop could be “listening in” on your every request for information, and the information you receive. This is the reason you are always counseled to never do anything with your financial apps, or any app that accesses personal private data, when you are in a coffee shop setting. The Wi-Fi routers at most of these locations are usually “Open” and not protected. Though the person at the next table is probably not listening to your communications, you should consider all open Wi-Fi communications as if it was available to the public.

So, at home where you will want to use your financial apps, it is important that you secure your Wi-Fi by employing encryption. This guarantees that your Wi-Fi communications cannot be compromised, even if someone with sniffer equipment parks in your driveway where the signal is strong enough to be intercepted. I would bet that most of us already have our Wi-Fi encrypted. Any Wi-Fi that requires a password is using some type of encryption and is therefore protected. Today, there are at least three types of encryption that are used with routers, WEP, WPA, and WPA2. WEP is the oldest and least secure way to encrypt your Wi-Fi, short of leaving it open or unencrypted. A WEP, or “Wired Equivalent Privacy”, password is said to be easy to crack, by those who practice the art of cryptography. WEP will only stop the most casual of users from connecting to a WEP protected network. Common advice is that if your router only supports WEP, you should replace it, post haste. All networks should use one of the stronger encryptions techniques, WPA or WPA2.

WPA or “Wi-Fi Protected Access” is the newer Wi-Fi security standard. There are two versions of WPA - WPA and WPA2. WPA was created as a stop gap solution for devices that originally only supported WEP. It allowed those devices to upgrade to a stronger encryption scheme, WPA, and leave behind the known flaws of WEP. WPA was always only a temporary solution improving the situation, but not expected to be the final solution. The final solution is WPA2. WPA2 is the most secure type of encryption available today for typical home equipment. (The government may have other encryption schemes but that would only be known by people way above my pay grade.) WPA2 is the encryption standard that we should all use on our routers at home. The strength of an encryption scheme comes from the algorithms used and the length of the encryption key. Without getting into the technical details, WPA2 uses the strongest algorithm and employs very long keys. The WPA2 in this discussion is sometimes called WPA2-Personal. There are other variants of WPA called WPA2-Enterprise that may be even more secure but are intended for large business installations. So, at home when you are setting up your typical home or small business router, make sure your data is protected, (and access to your Wi-Fi is limited), by setting up and using WPA2 Wi-Fi security.